(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 089 524 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.04.2001 Bulletin 2001/14

(51) Int Cl.[7]: **H04L 29/12**, H04L 12/28, H04L 29/06

(21) Application number: **00308550.3**

(22) Date of filing: **28.09.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **01.10.1999 US 411012**

(71) Applicant: **Web TV Networks Inc.**
Mountain View, California 94043 (US)

(72) Inventors:
- **Schmuelling, Guenther**
  San Jose, California 95123 (US)
- **Sears, Jr., Stephan Bartlett**
  Campbell, California 95008 (US)

(74) Representative: **Belcher, Simon James**
Urquhart-Dykes & Lord
Tower House
Merrion Way
Leeds LS2 8PA (GB)

(54) System for supporting multiple Internet service providers on a single network

(57) Described are methods and apparatus that allow cable customers who wish to add a cable modem (or other device) to a local network to choose both the cable modem through which they access the Internet and the Internet Service Provider (ISP) that will provide them that access. A system of hardware connects the local network to the Internet. This hardware includes cable-modem infrastructure that denies Internet access to devices on the local network that are not registered with an authorized ISP. The hardware also facilitates the registration process, allowing devices new to the local network to establish Internet-access agreements with ISPs, and thereby gain access to the Internet.

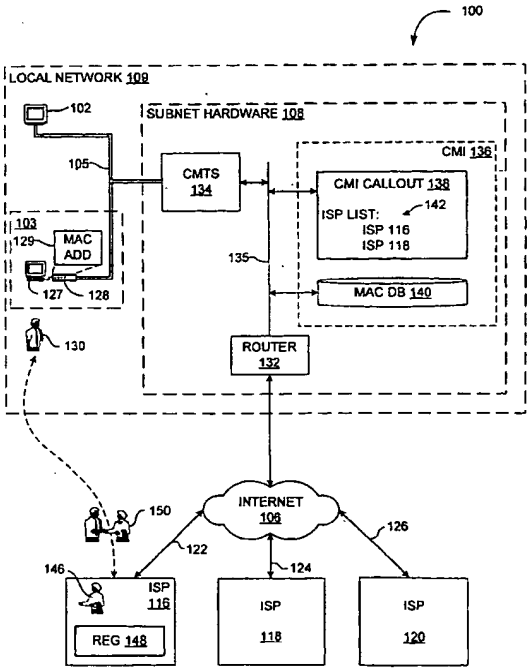

FIG. 1

EP 1 089 524 A2

Best Available Copy

Description

TECHNICAL FIELD

[0001] The invention relates to network-device registration systems that allow devices on a local network, such as a cable network, to register with Internet service providers to obtain access to the Internet.

BACKGROUND OF THE INVENTION

[0002] Cable modems handle incoming and outgoing data signals between a cable provider and a personal or business computer or television set. Cable modems are quickly replacing telephone modems in many areas because of the cable modem's superior bandwidth.

[0003] DOCSIS (Data Over Cable Systems Interface Specifications) is an industry standard that specifies an interface for cable modems. More specifically, DOCSIS specifies modulation schemes and protocols for exchanging bi-directional signals between devices on a cable network and devices on a TCP/IP network, typically the Internet.

[0004] DOCSIS describes a method by which a cable modem can receive an IP address to gain connectivity to the Internet. This method is sufficient for the simple case where the cable provider supplies cable modems to cable customers, who then access the Internet through an Internet Service Provider (ISP) specified by the cable provider. However, there is no provision for cable customers to receive IP addresses for cable modems that are not supplied by their cable provider. Moreover, there is no provision for allowing cable customers to select from among several ISPs on a single cable network. There is therefore a need for a system that allows cable customers to choose both the cable modem through which they access the Internet and the ISP that will provide them that access.

SUMMARY OF THE INVENTION

[0005] The present invention is directed to methods and apparatus that let cable customers who wish to add a cable modem (or other device) to a local cable network choose both the cable modem through which they access the Internet and the ISP that will provide them that access.

[0006] A system of hardware configured in accordance with one embodiment of the invention connects the local network to the Internet. This hardware includes cable-modem infrastructure (CMI) that denies Internet access to devices on the local network that are not registered with an ISP authorized by the cable company. The hardware also facilitates the registration process, allowing devices new to the local network to establish Internet-access agreements with ISPs, and thereby gain access to the Internet.

[0007] Every network device, including cable modems, has a unique identification code called a media-access control (MAC) address. New devices connected to the local network send their MAC address out onto the local network in an effort to obtain a routable IP address (i.e., an IP address that can be used to gain access to the Internet). The CMI intercepts such requests and looks in a MAC database to determine whether the device associated with the MAC address is registered with an ISP, and is therefore entitled to a routable IP address. If the MAC address is not listed, the CMI assigns the modem a non-routable address that can be used on the local network, but cannot be used to gain access to the Internet. The unregistered device can then use the non-routable address to communicate with a registration server in the CMI. The registration server is adapted to facilitate communication between the device and a selected ISP.

[0008] Using the non-routable IP address and the registration server, a user of the network device enters into an agreement with a selected ISP. The selected ISP sends a message to the CMI identifying the device, the ISP, and the existence of the service agreement. The CMI then modifies the MAC database to indicate that the device is now registered. The CMI responds to subsequent address requests from the now-registered device with a routable IP address.

[0009] Other features of the present invention will be apparent from the accompanying drawings and from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Figure 1 depicts a system 100 configured in accordance with the invention to facilitate communication between each of a pair of clients 102 and 103 on a cable subnet 105 and information resources available on the Internet 106.

[0011] Figure 2 is a flowchart 200 depicting a process of initiating a service agreement between a prospective Internet user and an Internet service provider.

[0012] Figure 3 depicts another system 300 configured in accordance with the invention to facilitate bi-directional communication between clients 102 and 103 and information resources available on the Internet 106.

[0013] Figure 4 is a flowchart 400 depicting a process of initiating a service agreement between a prospective Internet user and an Internet service provider.

[0014] Figure 5 is a flowchart 500 depicting the process of Figure 4 from the perspective of a client controlled by the prospective user.

DETAILED DESCRIPTION OF THE INVENTION

[0015] Figure 1 depicts a system 100 configured in accordance with the invention to facilitate bi-directional communication between each of a pair of clients 102 and 103 on a cable subnet 105 and resources available on the Internet 106 (or some other network or collection

of networks).

[0016] Cable subnet 105 connects to the Internet 106 via subnet hardware 108. In accordance with the invention, subnet hardware 108 enables clients 102 and 103 to register for Internet service with one of a number of Internet service providers (ISPs) 116, 118, and 120. ISPs 116, 118, and 120 connect to the Internet 106 via respective connections 122, 124, and 126. Cable subnet 105 and subnet hardware 108 collectively form a local network 109 through which clients 102 and 103 can access the Internet 106.

[0017] Client 102 is a set-top box equipped with an internal cable modem; client 103 includes a personal computer 127 connected to cable subnet 105 using an external cable modem 128. Each of clients 102 and 103 conventionally contains a unique media-access control (MAC) address, though only MAC address 129 for client 103 is shown. A computer user 130 is responsible for contracting with an ISP to receive Internet access via client 103.

[0018] Subnet hardware 108 includes a conventional router 132 connected to a conventional Cable Modem Termination System (CMTS) 134 via a TCP/IP subnet 135. A detailed discussion of CMTS 134, sometime referred to as a cable network "headend," is beyond the scope of the present disclosure. It is enough to note that CMTS 134 facilitates bi-directional information transfer between cable 105 and a TCP/IP network, such as the Internet 106. For a detailed discussion of CMTS 134, see the document entitled "Cable Modem Termination System-Network Side Interface Specification," SP-CMTS-NSII01-960702 (1996), which is incorporated herein by reference.

[0019] In accordance with the invention, subnet hardware 108 additionally includes cable-modem infrastructure (CMI) 136 connected to both CMTS 134 and router 132 via subnet 135. CMI 136, in turn, includes a MAC database 140, listing which clients on local network 102 are registered with an ISP, and a CMI callout 138 that bars unregistered devices from accessing the Internet and that allows unregistered devices to register for Internet service with authorized ISPs. Authorized ISPs are listed in CMI callout 138 as ISP list 142.

[0020] In the present example, ISP list 142 lists only ISP 116 and 118. The remaining ISP 120 is not authorized to provide service to clients on cable subnet 105, perhaps because the administrator of ISP 120 has not contracted with the administrator of local network 109 to provide service to clients on local network 109.

[0021] The dashed line delineating the boundary of local network 109 includes clients 102 and 103 and subnet hardware 108. Strictly speaking, however, local network 109 only includes cable subnet 105, CMTS 134, and TCP/IP subnet 135. Router 132 defines the boundary between local network 109 and the Internet 106.

[0022] ISP 116 includes an administrator 146 and an ISP registry 148. Administrator 146 can be either human or an automated user interface with which user 130 can establish an Internet-service agreement 150, illustrated as a "handshake" between administrator 146 and user 130. ISPs 118 and 120 may have administrators and registration databases similar to those of ISP 116.

[0023] Figure 2 is a flowchart 200 depicting a process of initiating service agreement 150 of Figure 1 between user 130 and administrator 146 of ISP 116, also of Figure 1. Such an agreement typically affords user 130 access to Internet resources via client 103. (Incidentally, the first digit of each reference number in this document corresponds to the number of the figure in which the identified element was first introduced.)

[0024] Beginning at step 202, modem 128 and CMTS 134 employ conventional protocols to communicate over cable subnet 105. CMTS 134 converts between RF signals on cable subnet 105 and digital signals that can be understood by devices on subnet 135. Having established communication with subnet 135, modem 128 transmits a message that includes MAC address 129. CMI callout 138 intercepts this message and determines whether modem 128 is registered with an ISP, and therefore has access to the Internet 106. CMI callout 138 makes this determination by looking to MAC database 140 for an entry identifying MAC address 129 (decision 204). If the answer is yes, then CMI 136 provides modem 128 with an IP address selected from a pool of ISP addresses stored within CMI callout 138.

[0025] If MAC 129 is not registered, then CMI callout 138 provides modem 128 with a non-routable IP address (step 208). The non-routable IP address allows modem 128 to communicate with resources on subnet 135; however, router 132 blocks modem 128 from communicating over the Internet 106. CMI callout 138 then stores MAC address 129 and the corresponding non-routable IP address in database 140 (step 210).

[0026] CMI server will receive one of two requests from client 103, depending upon whether additional devices within client 103 require an IP address. Computer 127 is a network device, and therefore requires its own IP address. Computer 127 typically transmits an address request a number of times before CMI 136 provides modem 128 with an IP address, thereby enabling modem 128 to communicate requests from computer 127. Upon receiving an address request from computer 127 (step 211), the process returns to decision 204. Computer 127 will then go through steps 208 and 210 as described above for modem 128.

[0027] Once modem 128 and 127 have been through steps 208 and 210, both devices have non-routable IP addresses that can be used to communicate with entities on local network 109. User 130 then begins the registration process by starting the browser on computer 127 and directing the browser to connect to a login page stored in CMI 136. This connection initiates a registration request to CMI 136 (step 211). The address of the login page might be provided to user 130 in the installation instructions for modem 128 or by the company that controls local network 109. In another embodiment,

the browser of computer 127 is factory configured to automatically connect to the appropriate login page when started.

[0028] CMI 136 responds to the registration request of step 211 by sending ISP list 142 to client 103 (step 212) and facilitating communication between client 103 and a selected ISP (step 214). CMI 136 thus enables user 130 to register client 103 with an ISP on the Internet 106 without requiring client 103 have a routable IP address.

[0029] The next two steps 216 and 218 are set out with dashed lines to emphasize that they are not separate steps performed by CMI 136, but are instead accomplished between user 130 and administrator 146 of ISP 116 during step 214. User 130 selects an ISP from ISP list 142 (step 216) and completes an Internet-service agreement with the administrator of the selected ISP (step 218). For illustrative purposes, user 130 is assumed to have selected ISP 116 and entered into agreement 150 with administrator 146.

[0030] Once user 130 and administrator 146 finalize agreement 150, then administrator 146 notes the agreement in registry 148 and notifies CMI 136 that computer 127 is registered. Upon receipt of this notice (step 220), CMI callout 138 modifies the entry in database 140 corresponding to the MAC address of computer 127 (step 222) to indicate that computer 127 is registered with the selected ISP. CMI 136 also requests that computer 127 release its non-routable IP address and request a new one (step 224). Computer 127 complies with these requests, returning the process to step 203. With computer 127 registered, subsequent requests from computer 127 for IP addresses pass through decision 204 to step 226, in which computer 127 receives a routable IP address.

[0031] In the embodiment of Figure 2, modem 128 does not communicate with devices outside of local network 109, and consequently need not register with an ISP to receive a routable IP address. In other embodiments, modem 128 registers to receive a routable IP address and then uses that address to provide Internet access to any number of devices, such as collection of computers like computer 127. In that embodiment, modem 128 acts as a DHCP server that provides local IP addresses for each of the computers. Modem 128 then translates these local IP addresses to the routable IP address assigned to modem 128 during the registration process. Thus, from the perspective of devices outside of client 103, modem 128 and the associated collection of computers appear as a single device with a single MAC address and a single IP address.

[0032] In another embodiment, CMI callout 138 communicates with CMTS 134 to receive a service-flow identifier (SFID) associated with modem 128. All devices behind modem 128 (e.g., computer 127) then automatically use the same SFID as modem 128. When CMI callout 138 receives a new DHCP request, callout 138 requests the SFID associated with the requesting device from CMTS 134; if that SFID matches one for a registered modem, then CMI callout 138 provides a routable IP address. Otherwise, the requesting device is directed through the registration process discussed above. Thereafter, modem 128 will be marked in database 140 as registered, which will allow all devices behind the modem to receive routable IP addresses.

[0033] Figure 3 depicts a system 300 configured in accordance with the invention. Various elements of Figure 3 were described above in connection with Figure 1, like-numbered elements being similar. For example, cable subnet 105, the Internet 106, and each component connected directly to cable subnet 105 and the Internet 106, are identical to the like-numbered elements of Figure 1.

[0034] In system 300, subnet hardware 302 facilitates communication between devices on cable subnet 105 and devices on the Internet 106. Subnet hardware 302 includes the same conventional router 132 and CMTS 134 described in connection with Figure 1. Subnet hardware 302 and cable subnet 105 are parts of a local network 303 controlled by e.g. a local cable company. Router 132 defines the boundary between local network 303 and the Internet 106.

[0035] Subnet hardware 302 includes cable-modem infrastructure (CMI) 304, a network administration interface 306, and a billing system 308, all interconnected by a TCP/IP subnet 312. CMI 304 includes a registration server 314, a DHCP server 316, a simple DNS server 317, a TIME daemon 318, a TFTP daemon 320, a SYSLOG daemon 322, a cache 326, a CMI database 328, and a DHCP callout 330.

[0036] DHCP stands for "Dynamic Host Configuration Protocol." DHCP server 316 passes configuration data and reusable network addresses to clients 102 and 103. DHCP server 316 uses a standard protocol specified in Request for Comment (RFC) 2131, entitled "Dynamic Host Configuration Protocol," by R. Droms (March 1997), which is incorporated herein by reference.

[0037] DCHP callout 330 is an Application Program Interface (API) that intercepts address requests from clients 102 and 103 directed to DHCP server 316, and intercepts responses from DHCP server 316 directed to clients 102 and 103. DHCP callout 330 caches messages from clients 102 and 103 in cache 326 to avoid unnecessary database lookups in response to redundant client requests. DHCP callout 330 includes a list 331 of ISPs with which clients on local network 303 may enter into a service agreement. Callout 330 bars unregistered devices from accessing the Internet and allow unregistered devices to register for Internet service. In the present example, DHCP callout 330 lists only ISPs 116 and 118. DHCP callout 330 additionally includes a local address pool 332 of non-routable IP addresses and an IP address pool 333 with IP addresses for use with each listed ISP. DCHP callout 330 is described below in more detail in connection with Figure 4.

[0038] "TIME" daemon 318 provides the time and

date to network clients so that cable modems do not require battery operated clocks. "Daemon" is a conventional term used to describe a program that is activated, when needed, without user intervention. TIME daemon 318 uses a standard protocol specified in RFC 868, entitled "Time Protocol," by J. Postel and K. Harrenstien (May 1983), which is incorporated herein by reference.

[0039] "TFTP" stands for "Trivial File Transfer Protocol." TFTP daemon 320 implements a simple file-transfer service that CMI 304 uses to provide configuration files to clients 102 and 103. TFTP daemon 320 uses a standard protocol specified in RFC 1350, entitled "The TFTP Protocol (Revision 2)" by K. Sollins (July 1992), which is incorporated herein by reference.

[0040] SYSLOG daemon 322 provides a standard Application Program Interface (API) that allows clients 102 and 103 to log errors in a single location. For example, once modem 128 receives an IP address, modem 128 will send error messages over local network 303 to SYSLOG daemon 322 for logging. This allows administrator 306 to check for error messages in a single location.

[0041] CMI database 328 defines a number of fields that correlate MAC addresses from network clients with information specific to each client. For example, CMI database 328 lists, for each registered client, the type of modem, the ISP with which the client is registered, and the client's billing status. A specific embodiment of database 328 is detailed in "Cable Modem Infrastructure Guide, Microsoft® TV Server 1.0 Deployment Pre-Release," from WebTV Networks, Inc. (September 29, 1999 - 3pm), which is incorporated herein by reference.

[0042] Figure 4 is a flowchart 400 depicting a process of initiating service agreement 150 (Figures 1 and 3) between user 130 and administrator 146 of ISP 116. Beginning at step 401, modem 128 and CMTS 134 establish communication between subnet 105 and TCP/IP subnet 312. Modem 128 then transmits a DHCP discover message asking for DHCP servers on local network 303. DHCP callout 330 receives and intercepts the discover message (step 402), which includes MAC address 129, and checks to see whether MAC address 129 is listed in database 328 (decision 404).

[0043] Assuming that modem 128 is new to local network 303 -- and therefore that MAC address 129 is not listed in database 328 -- DHCP callout 330 adds MAC address 129 and some default modem settings to both database 328 and cache 326 (step 408). Caching MAC 129 and the default settings speeds step 404 in the event that CMI 304 receives more than one discover message from modem 128. Such a repeat message might occur during high load situations or when a malicious user attempts to disrupt local network 303 by sending a stream of repeat messages.

[0044] DHCP server 316 responds to the DHCP discover message with a DHCP offer message (step 410) that includes an available non-routable IP address from local address pool 332 and conventional configuration parameters for use by modem 128. Modem 128 responds to the DHCP offer message by broadcasting a DHCP request message addressed to DHCP server 316. DHCP server 316 then receives the request message (step 414) and returns a DCHP response message to modem 128 (step 416). The DCHP response message provides modem 128 with configuration parameters, including a committed non-routable IP address from local address pool 332 and the IP addresses of devices on local network 303 with which modem 128 may have to communicate. Such devices include simple DNS server 317, time daemon 318, tftp daemon 320, and syslog daemon 322. Once modem 128 receives these parameters, modem 128 accesses the addressed devices to obtain configuration information and, in the case of syslog daemon 322, to report any errors. This completes the boot process of modem 128, leaving modem 128 able to communicate information to and from computer 127. CMI callout 138 then flushes cache 326 (step 417) and stores the assigned IP address and default configuration data in database 328 (step 418) with MAC address 129.

[0045] A device behind cable modem 128 may require an additional IP address. In the present example, computer 127 needs an IP address and will therefore issue a DHCP discover request. Computer 127 may issue this request a number of times before modem 128 receives an IP address enabling modem 128 to convey the request from computer 127. Upon receiving DHCP discover message from computer 127 (step 419), the process returns to decision 404.

[0046] In the example, computer 127 is not registered. Thus, the MAC address of computer 127 is not listed in cache 326 or database 328. Consequently, computer 127 proceeds from step 408 through step 418 in the same manner that modem 128 traversed those steps. Thus, the second time the process arrives at step 419, both modem 128 and computer 127 are listed in database 328.

[0047] At this point, both modem 128 and computer 127 have non-routable IP addresses that can be used to communicate with entities on local network 303. Further, computer 127 has been provided with the addressing information required for computer 127 to communicate with various elements of CMI 304, including registration server 314.

[0048] User 130 begins the registration process by starting the browser on computer 127 and, if the browser is not configured to do so automatically, directing the browser to connect to a login page, http://login, in one embodiment. Earlier (step 416), the DHCP response message set the DNS server entry in computer 127 to simple DNS 317. The hostname "login" on simple DNS server 317 points to the self-registration page on registration server 314. Thus, when user 130 starts the browser on the unregistered client 103, the browser automatically connects to the self-registration page. When the browser connects, registration server 314 requests

a token and ISP list 331 from DHCP callout 330. The token is a key given to client 103 to present to an ISP when registering with the ISP. The ISP will have to present the token back to CMI 304 to authenticate that client 103 registered with the ISP. The use of a token thus ensures that user 130 entered into a service agreement with the ISP. In one embodiment, the token is a 64-bit random number.

[0049] From step 419, callout 330 presents the requested token and ISP list 331 to registration server 314 and stores the token in database 328 with the MAC address of computer 127 (step 422). Registration server 314 then forwards the token and ISP list 131 to computer 127 and prompts user 130 to select from among the listed ISPs. Upon selecting an ISP, user 130 is presented with the registration page of the selected ISP (e.g., a page in registry 148 of- ISP 116) by way of registration server 314. In effect, registration server 314 acts as a TCP/IP proxy and routes data between client 103 and ISP 116.

[0050] Registry 148 prompts user 130 for registration data and requests a list of available IP and service classes from CMI 304. Registry 148 then presents the available IP and service classes to user 130, who then selects a service class from the list. IP classes are used when a single ISP has multiple pools of IP addresses. Addresses from different pools may be routed differently, through better network connections, for example. Service classes specify what level of service a user receives within a given pool of IP addresses. For example, a particular user may receive higher priority than others in the same IP class.

[0051] Once user 130 and administrator 146 finalize agreement 150, administrator 146 adds the MAC address for computer 127 to ISP registry 148 and notifies CMI 136 that computer 127 is registered. The notice from ISP registry 148 includes the token and various required ISP settings. Callout 138 receives this message and, if the token is the same one originally supplied to computer 127, modifies the entry in database 328 corresponding to computer 127 (step 426) to include the ISP settings and to indicate that computer 127 is registered with the selected ISP.

[0052] Upon completion of the registration process, callout 330 requests that computer 127 release and re-request its IP address (step 428). Computer 127 thus releases its non-routable IP address and transmits a new DHCP discover message. Callout 330 receives the DHCP request (step 203) and again examines the MAC entry of computer 127 to determine whether computer 127 is listed in database 328. Because computer 127 was so listed in step 408, the process moves to step 430 in which callout 330 determines whether computer 127 is listed in database 328 as "blocked."

[0053] A particular client or device may be listed as "blocked" for many reasons. For example, an administrator in the local cable company controlling local network 303 might block access from a device found to be distributing illegal or offensive content, or a member of the cable company's billing department might block access to cable subscribers who are unwilling to pay for the service. Administration interface 306 and billing-system interface 308 are Component Object Model (COM) interfaces that afford cable-company employees access to database 328 for these and other purposes.

[0054] If computer 127 is not blocked, CMI callout 330 examines a second field in database 328 corresponding to the respective MAC address, this time to determine whether computer 127 is registered with an ISP (decision 432). In the example, computer 127 is registered with ISP 116, so callout 330 issues computer 127 a routable IP address from address pool 333. Had computer 127 not been registered, then the process flow would move to step 410 and would continue as described above. A client might be listed in database 328 but not registered if, for example, the user did not complete a registration process. Alternatively, a user or an ISP might send a message to registration server 314 indicating the cessation of a registration agreement between the user and the ISP. Registration server 314 could then mark the user's client as unregistered without removing the associated MAC address from database 328.

[0055] Figure 5 is a flowchart 500 depicting the process of initiating service agreement 150 between user 130 and administrator 146 of ISP 116 from the perspective of client 103. Beginning at step 501, modem 128 and CMTS 134 communicate over cable subnet 105 to establish a connection between cable subnet 105 and TCP/IP subnet 312. Modem 128 then transmits a DHCP discover message (step 502) asking for DHCP servers on local network 303. Modem 128 can expect one of three responses:

1. if modem 128 is registered with an ISP, then modem 128 will receive a DHCP offer message containing a fully routable IP address (step 504) from address pool 333;
2. if CMI 304 lists modem 128 as a blocked device, then modem 128 will receive an error message 509 from CMI 304; and
3. if modem 128 is not registered with an ISP, then modem 128 will receive a DHCP offer message (step 510) from CMI 304 containing a non-routable IP address.

The offer message of step 510 includes a non-routable IP address from local address pool 332 and some configuration parameters for modem 128. Modem 128 responds to the offer message by sending a DHCP request message (step 514) addressed to DHCP server 316. DHCP server 316 of CMI 304 returns a DCHP response message to modem 128 (step 516). As mention above in connection with Figure 4, the DCHP response message provides modem 128 with configuration parameters, including a committed non-routable IP ad-

dress and the IP addresses of devices on local network 303 with which modem 128 may have to communicate. Modem 128 then contacts various resources on local network 303 using the configuration parameters (step 518). These resources include time, tftp, and syslog daemons 318, 320, and 322. During this process, modem 128 contacts:

1. time daemon 318 to get the time;
2. tftp daemon 320 to get a modem configuration file;
3. syslog daemon 322, as necessary, to report any errors; and
4. simple DNS server 317 to get the address of registration server 314, which contains the self-registration page.

What client 103 does after step 518 depends on whether there are additional devices within client 103 that need IP addresses.

[0056] If another device, such as computer 127, requires an IP address, then that other device will send its own DHCP discover message (decision 520) and traverse flowchart 500 in the manner described above for modem 128. Assuming that computer 127 requires an IP address, the process proceeds once again through the steps on the left-hand side of flowchart 500 to step 518. Both modem 128 and computer 127 then have non-routable IP addresses that can be used to communicate with entities on local network 303. Once each device within client 103 has a non-routable IP address, the registration process begins when user 130 starts the browser on computer 127 (step 521).

[0057] The browser connects to its login page, http://login, either automatically or as directed by user 130 (step 522). Registration server 314 then requests and receives a token and ISP list 331 from DHCP callout 330. Registration server 314 then sends the token and list to computer 127. Having received the token and ISP list 331 (step 523), user 130 selects from among the listed ISPs (step 524). Registration server 314 facilitates communication between client 103 and the selected ISP so that user 130 can register computer 127 with the selected ISP.

[0058] Once registered, computer 127 receives a request from CMI 304 instructing computer 127 to release the assigned IP address and request another (step 526). Computer 127 then releases its non-routable IP address (step 528) and acquires a new IP address by issuing a new DHCP discover message (returning to step 502). Because computer 127 is now registered, CMI 304 responds to the DHCP discover message with a routable IP address (step 504) that allows computer 127 to access the Internet 106.

[0059] While the present invention has been described in connection with specific embodiments, variations of these embodiments will be apparent. For example, while described in connection with cable-modem networks, the invention is equally applicable to other types of local networks. Therefore, the spirit and scope of the appended claims should not be limited to the foregoing description.

Claims

1. A method for initiating a service agreement between a user of a network device on a first network and one of a plurality of service providers having corresponding servers on a second network, wherein the network device includes an identification code unique to the first network, the method comprising:

   a. receiving the code from the network device;
   b. transmitting a message to the network device, the message including a list of the service providers;
   c. prompting the user to select one of the service providers and establish the service agreement with the selected one of the service providers; and
   d. receiving a notice from the selected one of the service providers, the notice identifying the network device and the selected one of the service providers.

2. The method of claim 1, further comprising storing at least a portion of the notice.

3. The method of claim 1, further comprising receiving a request for a second address unique on the first and second networks before (a), and refusing the request until after (d).

4. The method of claim 1, wherein the notice includes the code.

5. The method of claim 1, wherein the message to the network device includes a token, and wherein the notice from the selected one of the service providers also includes the token.

6. A method for initiating a service agreement between a user of a network device on a first network and a service provider on a second network, wherein the network device includes at least one identification code unique to the first network, the method comprising:

   a. receiving the code from the network device;
   b. assigning a local IP address to the network device;
   c. transmitting the code and the local IP address to the network device, the local IP address allowing the network device to communi-

cate with at least one of a first plurality of devices on the first network, but not allowing the network device to communicate with a second plurality of devices on the second network;
d. prompting the user to establish the service agreement with the service provider;
e. receiving a notice from the service provider, the notice identifying at least one of the network device and the user of the network device; and
f. assigning a global IP address to the network device, the global IP address allowing the network device to communicate with the second plurality of devices on the second network.

7. The method of claim 6, further comprising prompting the user to select the service provider from a plurality of service providers.

8. The method of claim 6, further comprising storing the code and a second code identifying the service provider after (e).

9. A local network system comprising:

a. a plurality of cable modems connected to one another via a cable network, each of the modems including a corresponding unique identifier;
b. a network headend having a first network node connected to the cable network and a second network node;
c. an address server connected to the second network node of the headend, the address server including a modem database adapted to store the identifiers of the cable modems;
d. a router connected between the local network and a second network;
e. an ISP server connected to the router via the second network.

10. The local network system of claim 9, wherein the headend is a CMTS headend.

11. The local network system of claim 9, wherein the address server is a DHCP server.

12. A system for establishing communication between a network computer connected to a local network and a remote information store connected to a second network, the system comprising:

a. a server connected to the local network and adapted to:

i. receive a unique identifier from the network computer and, in response, assign a non-routable address to the network computer, wherein the non-routable address is unique to the local network;
ii. facilitate an agreement between a user of the network computer and an entity authorized to grant the network computer access to the second network; and
iii. store the unique identifier in a database identifying the network computer as a registered network computer;

b. an address server connected to the local network and adapted to assign a routable IP address to the registered network computer.

13. The system of claim 12, wherein the local network comprises a cable network.

14. The system of claim 12, wherein the second network comprises the Internet.

15. The system of claim 14, wherein the entity authorized to grant the network computer access to the second network is an Internet Service Provider.

16. The system of claim 14, wherein the remote information store is an Internet resource.

17. A method of establishing communication between a network computer connected to a local network and a remote information store connected to a second network, the method comprising:

a. receiving a unique identifier from the network computer;
b. determining, based on the unique identifier from the network computer, whether the network computer has authority to access the second network; and
c. if the network computer lacks authority to access the second network,

i. providing a non-routable address to the network computer, wherein the non-routable address lacks authority to access the second network;
ii. facilitating an agreement between a user of the network computer and an entity authorized to grant the network computer access to the second network; and
iii. providing the network computer a routable address with authority to access the second network upon completion of the agreement.

18. A method of establishing communication between a network computer connected to a local network and a remote information store connected to a second network, the method comprising:

a. sending a unique identifier from the network computer;
b. receiving a non-routable address, wherein the non-routable address lacks authority to access the second network;
c. receiving, from a device on the local network, a list identifying a plurality of service providers on the second network; and
d. selecting one of the plurality of service providers.

19. The method of claim 18, further comprising receiving a token from the device on the local network and sending the token to the selected one of the plurality of service providers.

20. The method of claim 18, further comprising receiving a token from the device on the local network and sending the token to the selected one of the plurality of service providers through the device on the local network.

21. The method of claim 18, further comprising receiving a request to release the non-routable address after (d).

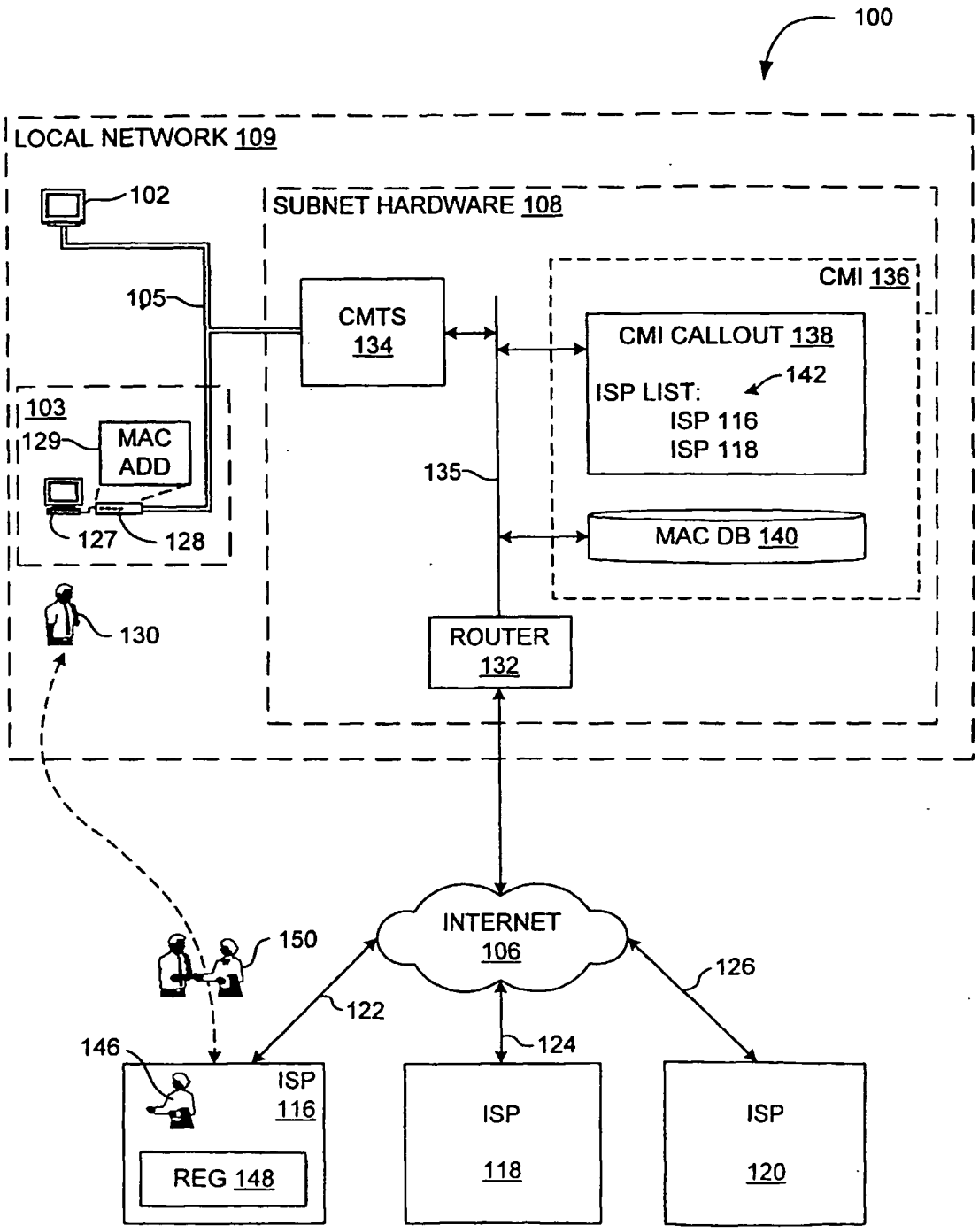
100
LOCAL NETWORK 109
102
SUBNET HARDWARE 108
105
CMTS
134
CMI 136
CMI CALLOUT 138
142
ISP LIST:
ISP 116
ISP 118
103
129
MAC
ADD
135
127
128
MAC DB 140
130
ROUTER
132
INTERNET
106
150
122
126
124
146
ISP
116
REG 148
ISP
118
ISP
120

FIG. 1

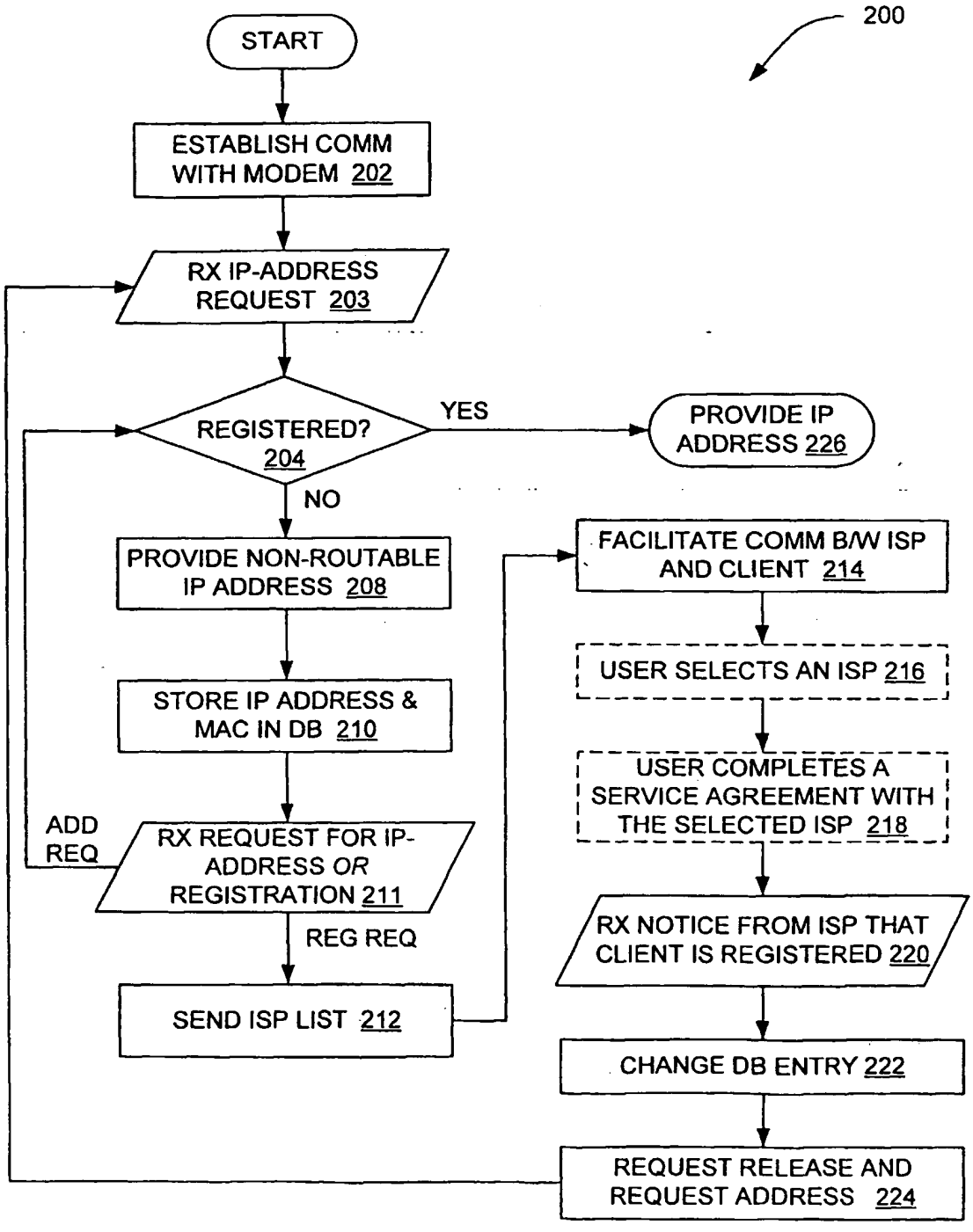
200
START
ESTABLISH COMM WITH MODEM 202
RX IP-ADDRESS REQUEST 203
REGISTERED? 204
YES
PROVIDE IP ADDRESS 226
NO
PROVIDE NON-ROUTABLE IP ADDRESS 208
STORE IP ADDRESS & MAC IN DB 210
ADD REQ
RX REQUEST FOR IP-ADDRESS OR REGISTRATION 211
REG REQ
SEND ISP LIST 212
FACILITATE COMM B/W ISP AND CLIENT 214
USER SELECTS AN ISP 216
USER COMPLETES A SERVICE AGREEMENT WITH THE SELECTED ISP 218
RX NOTICE FROM ISP THAT CLIENT IS REGISTERED 220
CHANGE DB ENTRY 222
REQUEST RELEASE AND REQUEST ADDRESS 224

FIG. 2

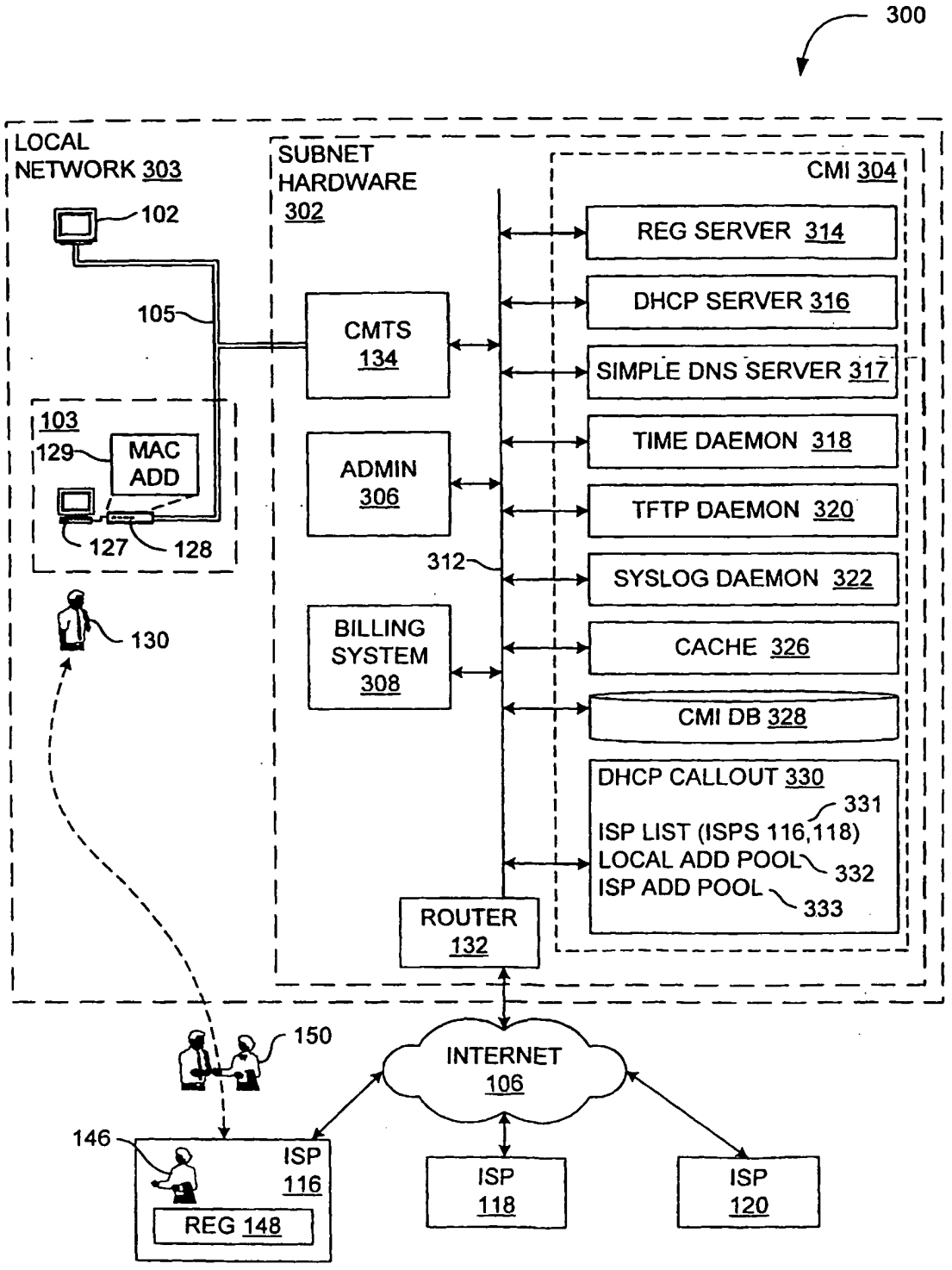
300
LOCAL NETWORK 303
SUBNET HARDWARE 302
CMI 304
102
105
CMTS 134
REG SERVER 314
DHCP SERVER 316
SIMPLE DNS SERVER 317
TIME DAEMON 318
TFTP DAEMON 320
SYSLOG DAEMON 322
CACHE 326
CMI DB 328
DHCP CALLOUT 330
331
ISP LIST (ISPS 116,118)
LOCAL ADD POOL
332
ISP ADD POOL
333
103
129
MAC ADD
127
128
130
ADMIN 306
312
BILLING SYSTEM 308
ROUTER 132
150
INTERNET 106
146
ISP 116
REG 148
ISP 118
ISP 120

FIG. 3

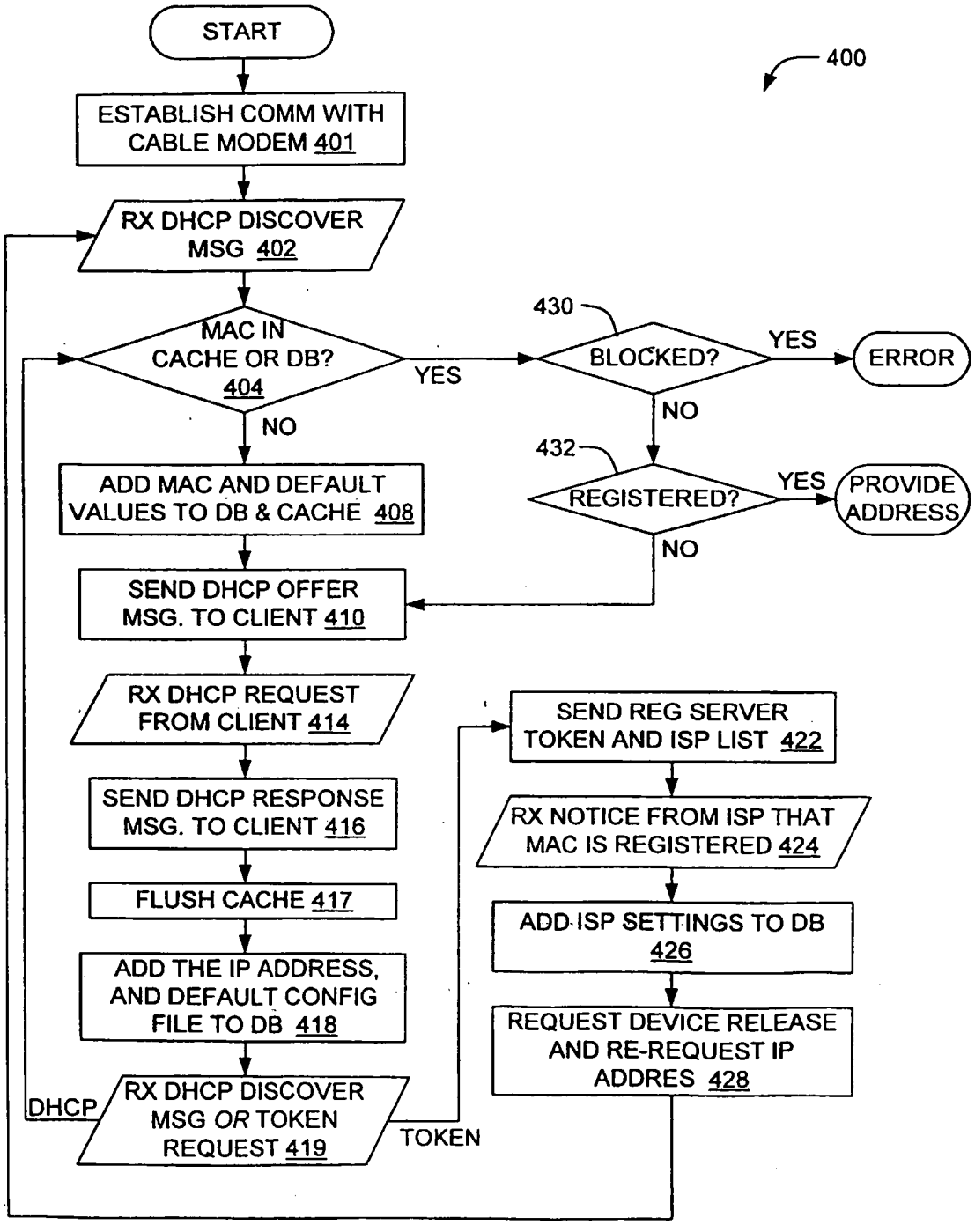
START
400
ESTABLISH COMM WITH CABLE MODEM 401
RX DHCP DISCOVER MSG 402
MAC IN CACHE OR DB? 404
YES
430
BLOCKED?
YES
ERROR
NO
432
REGISTERED?
YES
PROVIDE ADDRESS
NO
ADD MAC AND DEFAULT VALUES TO DB & CACHE 408
SEND DHCP OFFER MSG. TO CLIENT 410
RX DHCP REQUEST FROM CLIENT 414
SEND DHCP RESPONSE MSG. TO CLIENT 416
FLUSH CACHE 417
ADD THE IP ADDRESS, AND DEFAULT CONFIG FILE TO DB 418
DHCP
RX DHCP DISCOVER MSG OR TOKEN REQUEST 419
TOKEN
SEND REG SERVER TOKEN AND ISP LIST 422
RX NOTICE FROM ISP THAT MAC IS REGISTERED 424
ADD ISP SETTINGS TO DB 426
REQUEST DEVICE RELEASE AND RE-REQUEST IP ADDRES 428

FIG. 4

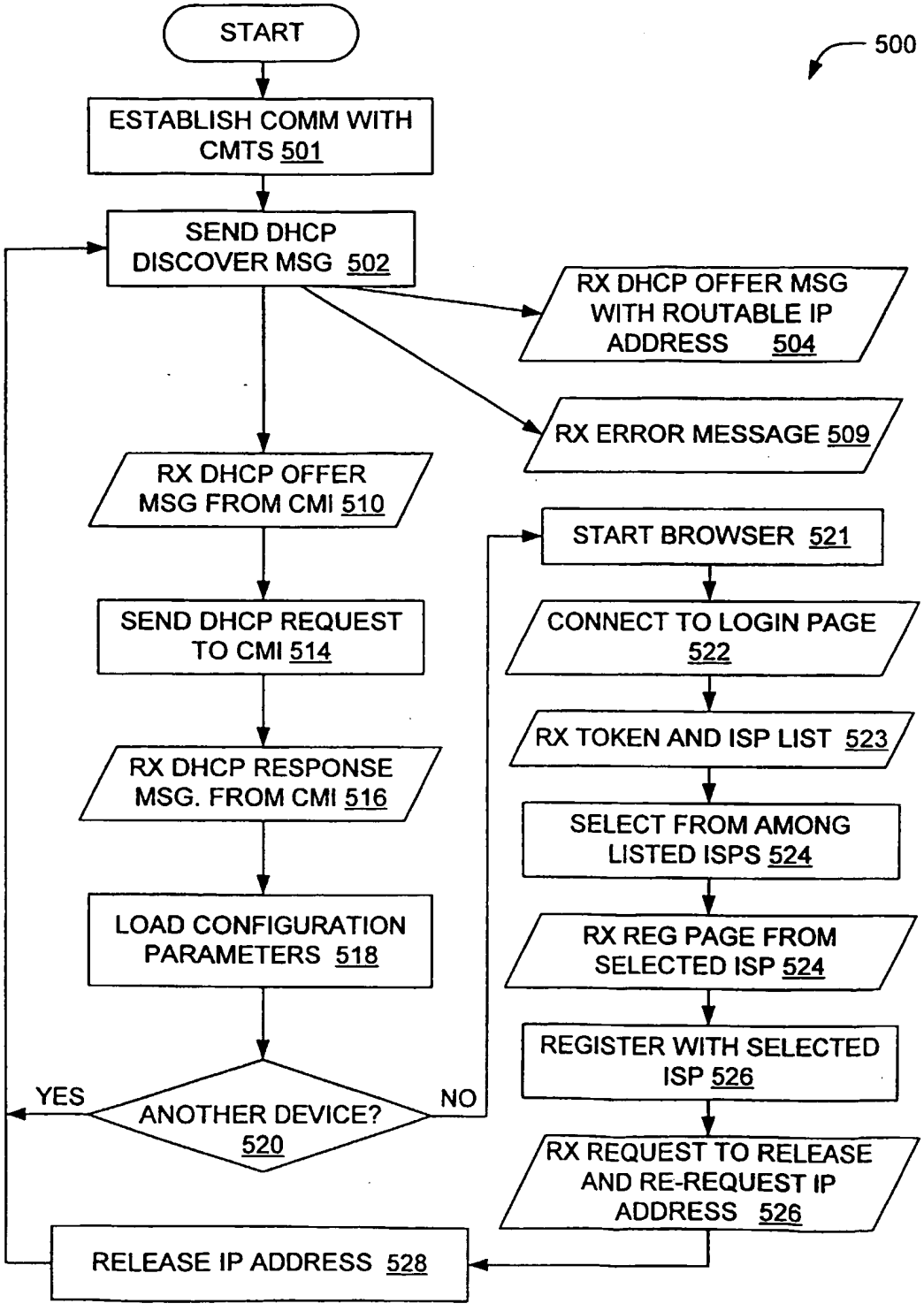
START
500
ESTABLISH COMM WITH CMTS 501
SEND DHCP DISCOVER MSG 502
RX DHCP OFFER MSG WITH ROUTABLE IP ADDRESS 504
RX ERROR MESSAGE 509
RX DHCP OFFER MSG FROM CMI 510
SEND DHCP REQUEST TO CMI 514
RX DHCP RESPONSE MSG. FROM CMI 516
LOAD CONFIGURATION PARAMETERS 518
YES
ANOTHER DEVICE? 520
NO
START BROWSER 521
CONNECT TO LOGIN PAGE 522
RX TOKEN AND ISP LIST 523
SELECT FROM AMONG LISTED ISPS 524
RX REG PAGE FROM SELECTED ISP 524
REGISTER WITH SELECTED ISP 526
RX REQUEST TO RELEASE AND RE-REQUEST IP ADDRESS 526
RELEASE IP ADDRESS 528

FIG. 5